

Notice of Allowability

Application No.

09/998,915

Examiner

Jude J. Jean-Gilles

Applicant(s)

VILLAVICENCIO, FRANCISCO J.

Art Unit

2143

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to 08/11/2006.
2. ☒ The allowed claim(s) is/are 1-7, 9-18, 20-24, 26-30, 32-36, 38-40, 42-46 and 48.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some* c) ☐ None of the:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. _____.
3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.


Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
- (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
- 1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
- (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date 08/11/2006
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☒ Interview Summary (PTO-413),
Paper No./Mail Date _____
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____


DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

EXAMINER'S AMENDMENT

1. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it **MUST** be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with DALEY WILLIAM J. Reg. No. 52,471 on September 22, 2006. The proposed amendment to the claims as suggested by the examiner, and agreed upon by DALEY WILLIAM J. to the Examiner on September 22, 2006 is presented below.

IN THE CLAIMS

2. In this proposed amendment, claims 8, 19, 25, 31, 37, 41, and 47 have been cancelled and independent claims 1, 16, 24, 28, 35, 39, and 45 have all been amended to include the steps of claims 8, 19, 25, 31, 37, 41, and 47 respectively. As such this application is now in condition for allowance and applicants still maintain the right to file one or more continuations on this application to seek broader and/or additional claims. Furthermore, claim 9, which depends upon claim 8, is now amended to depend upon amended claim 1.

PROPOSED EXAMINER'S AMENDMENTS TO THE CLAIMS:

1.(Currently amended) A method for impersonating, comprising the steps of: receiving authentication credentials for a first entity and an identification of a second entity;

authenticating said first entity based on said authentication credentials for said first entity;

creating a cookie that stores an indication of said second entity if said step of authenticating is performed successfully; and

authorizing said first entity to access a first resource as said second entity based on said cookie;

wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said second entity, and accessing one or more attributes of said second user identity profile; and

said cookie includes said one or more attributes of said second user identity profile.

2. (Previously Presented) A method according to claim 1, further comprising the step of: providing a form for said authentication credentials, said form includes a request for a user identification, a password and an impersonatee identification, said user identification and said password correspond to said authentication credentials for said first entity, said impersonatee identification corresponds to said identification of said second entity.

3. (Original) A method according to claim 1, wherein: said step of receiving is performed by an access system; said access system protects said first resource; and said first resource is separate from said access system.
4. (Original) A method according to claim 1, wherein: said step of receiving is performed by an access system; said access system protects a plurality of resources; and said plurality of resources includes said first resource.
5. (Previously Presented) A method according to claim 1, wherein: said cookie stores a distinguished name of said second entity and an IP address for said first entity.
6. (Previously Presented) A method accord to claim 1, further comprising the steps of: receiving a request to access said first resource; providing a form for said authentication credentials, said form includes a request for a user identification, a password and an impersonates identification, said user identification and said password correspond to said authentication credentials for said first entity, said impersonatee identification corresponds to said identification of said second entity; and transmitting said cookie for storage on a device being used by said first entity to send said request to access said first resource.
7. (Original) A method according to claim 1, wherein: said steps of receiving, authenticating and authorizing are performed by an access system; said access system

provides access management services and identity management services; and said first resource is protected by, but separate from, said access system.

8. (Cancelled)

9.(Currently amended) A method according to claim 8-7, wherein: said steps of searching a directory server for a first user identity profile and verifying said password based on said user identity profile are performed by a first authentication plug-in; and said steps of searching said directory server for a second user identity profile and accessing one or more attributes of said second user identity profile are performed by a second authentication plug-in.

10. (Previously Presented) A method according to claim 1, wherein:

said cookie stores a distinguished name for said second entity; and

said step of authorizing includes the steps of:

accessing said distinguished name stored in said cookie,

accessing a user identity profile for said second entity based on said distinguished name,

accessing a set of one or more authorization rules for said first resource,
and

comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said first resource.

11. (Previously Presented) A method according to claim 1, wherein: said authentication credentials correspond to a set of attributes for said first entity; said identification of said second entity corresponds to a set of attributes for said second entity; said step of authorizing is based on one or more of said attributes for said first entity; and said step of authorizing is based on one or more of said attributes for said second entity.

12. (Previously Presented) A method according to claim 1, wherein: said authentication credentials correspond to a set of attributes for said first entity; and said step of authorizing is not based on attributes for said first entity.

13. (Previously Presented) A method according to claim 1, further comprising the steps of: receiving a request for a login form; and providing said login form, said login form includes a request for a user identification, a password and an impersonatee identification, said user identification and said password correspond to said authentication credentials for said first entity, said impersonatee identification corresponds to said identification of said second entity.

14. (Previously Presented) A method according to claim 1, further comprising the steps of: receiving a request from said first entity to access a second resource after said step of creating said cookie; accessing contents of said cookie and determining not to authenticate said first entity in response to said request to access said second resource;

Art Unit: 2143

and authorizing said first entity to access said second resource as said second entity based on said cookie, said step of authorizing said first entity to access said second resource is performed without authenticating said first entity in response to said request to access said second resource.

15. (Previously Presented) A method according to claim 1, wherein: said steps of authenticating and authorizing are performed without knowing a password for said second entity.

16. (Currently amended) A method for impersonating, comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity at an access system, said access system protects a first resource that is separate from said access system;

authenticating said first entity based on said authentication credentials for said first entity, said step of authenticating is performed by said access system; and

authorizing said first entity to access said first resource as said second entity, said step of authorizing is performed by said access system;

wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,
verifying said password based on said user identity profile, searching said directory

Art Unit: 2143

server for a second user identity profile that matches said identification of said second entity, and accessing one or more attributes of said second user identity profile; and
said step of authorizing uses said one or more attributes of said second user identity profile.

17. (Previously Presented) A method according to claim 16, wherein: said steps of authenticating and authorizing are performed without knowing a password for said second entity.

18. (Previously Presented) A method according to claim 16, wherein: said access system protects a plurality of resources that are separate from said access system; and said plurality of resources includes said first resource.

19. (Cancelled)

20. (Original) A method according to claim 16, wherein: said steps of searching a directory server for a first user identity profile and verifying said password based on said user identity profile are performed by a first authentication plug-in; and s
said steps of searching said directory server for a second user identity profile and accessing one or more attributes of said second user identity profile are performed by a second authentication plug-in.

21. (Previously Presented) A method according to claim 16, wherein:

said step of authenticating provides a name for said second entity; and

said step of authorizing includes the steps of:

accessing said name,

accessing a user identity profile for said second entity based on said name,

accessing a set of one or more authorization rules for said resource, and

comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said resource.

22. (Previously Presented) A method according to claim 16, wherein:

said authentication credentials correspond to a set of attributes for said first entity;

said identification of said second entity corresponds to a set of attributes for said second entity;

said step of authorizing is based on one or more of said attributes for said first entity; and

said step of authorizing is based on one or more of said attributes for said second entity.

23. (Previously Presented) A method according to claim 16, further comprising the steps of: receiving a request to access a second resource from said first entity after said step

Art Unit: 2143

of authenticating said first entity, said access system protects said second resource;
and authorizing said first entity to access said second resource as said second entity,
said step of authorizing said first entity to access said second resource is performed
without authenticating said first entity in response to said request to access said second
resource.

24. (Currently Amended) A method for impersonating, comprising the steps of:

receiving authentication credentials for a first entity and an identification of a
second entity at an access system, said access system protects a plurality of resources;
receiving an indication of one or more of said plurality of resources;
authenticating said first entity based on said authentication credentials for said
first entity, said step of authenticating is performed by said access system; and
authorizing said first entity to access said one or more of said plurality of
resources as said second user, said step of authorizing is performed by said
access system;

wherein: said authentication credentials include an ID and a password; said step
of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID,
verifying said password based on said user identity profile, searching said directory
server for a second user identity profile that matches said identification of said second
entity, and accessing one or more attributes of said second user identity profile; and

said step of authorizing uses said one or more attributes of said second user identity profile.

25. (Cancelled).

26. (Original) A method according to claim 24, wherein:

said step of authenticating provides a name for said second entity; and said step of authorizing includes the steps of: accessing said name, accessing a user identity profile for said second entity based on said name, accessing a set of one or more authorization rules for said resource, and comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules.

27. (Original) A method according to claim 24, wherein: said authentication credentials correspond to a set of attributes for said first entity; said identification of said second entity corresponds to a set of attributes for said second entity; said step of authorizing is based on one or more attributes for said first entity; and said step of authorizing is not based on attributes for said first entity.

28. (Currently Amended) One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity;

authenticating said first entity based on said authentication credentials for said first entity;

creating a cookie that stores an indication of said second entity if said step of authenticating is performed successfully; and

authorizing said first entity to access a first resource as said second entity based on said cookie;

wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said second entity, and accessing one or more attributes of said second user identity profile; and
said cookie includes said one or more attributes of said second user identity profile.

29. (Original) One or more processor readable storage devices according to claim 28, wherein: said steps of receiving, authenticating and authorizing are performed by an access system; said access system protects a plurality of resources separate from said access system; and said plurality of resources includes said first resource.

Art Unit: 2143

30. (Previously presented) One or more processor readable storage devices according to claim 28, wherein:

said cookie stores a distinguished name of said second entity and an IP address for said first entity.

31. (Cancelled).

32. One or more processor readable storage devices according to claim 28, wherein:

said cookie stores a distinguished name for said second entity; and
said step of authorizing includes the steps of:
accessing said distinguished name stored in said cookie,
accessing a user identity profile for said second entity based on said distinguished name,
accessing a set of one or more authorization rules for said first resource, and
comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said first resource.

33. (Previously Presented) One or more processor readable storage devices according to claim 28, wherein: said authentication credentials correspond to a set of attributes for said first entity; said identification of said second entity corresponds to a set of attributes for said second entity; said step of authorizing is based on one or more of said attributes for said first entity; and said step of authorizing is based on one or more of said

attributes for said second entity.

34. (Previously Presented) One or more processor readable storage devices according to claim 28, wherein: receiving a request from said first entity to access a second resource after said step of creating said cookie; accessing contents of said cookie and determining not to authenticate said first entity in response to said request to access said second resource; and authorizing said first entity to access said second resource as said second entity based on said cookie, said step of authorizing said first entity to access said second resource is performed without authenticating said first entity in response to said request to access said second resource.

35. (Currently Amended) An apparatus for providing access management that allows for impersonating, comprising:

- a communication interface;

- a storage device; and

- a processing unit in communication with said communication interface and said storage device, said processing unit performs a method comprising the steps of:

 - receiving authentication credentials for a first entity and an identification of a second entity,

 - authenticating said first entity based on said authentication credentials for said first entity,

creating a cookie that stores an indication of said second entity if said step of authenticating is performed successfully, and

authorizing said first entity to access a first resource as said second entity based on said cookie;

wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said second entity, and accessing one or more attributes of said second user identity profile; and

said cookie includes said one or more attributes of said second user identity profile.

36. (original) An apparatus according to claim 35, wherein: said steps of receiving, authenticating and authorizing are performed by an access system; said access system protects a plurality of resources separate from said access system; and said plurality of resources includes said first resource.

37. (Cancelled).

38. (Previously Presented) An apparatus according to claim 35, wherein: said cookie stores a distinguished name for said second entity; and said step of authorizing includes

Art Unit: 2143

the steps of: accessing said distinguished name stored in said cookie, accessing a user identity profile for said second entity based on said distinguished name, accessing a set of one or more authorization rules for said first resource, and comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said first resource.

39. One or more processor readable storage devices having processor readable code embodied on said processor readable storage devices, said processor readable code for programming one or more processors to perform a method comprising the steps of:

receiving authentication credentials for a first entity and an identification of a second entity at an access system, said access system protects a first resource that is separate from said access system;

authenticating said first entity based on said authentication credentials for said first entity, said step of authenticating is performed by said access system; and

authorizing said first entity to access said first resource as said second entity, said step of authorizing is performed by said access system;

wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said second entity, and accessing one or more attributes of said second user identity profile; and

said step of authorizing uses said one or more attributes of said second user identity profile.

40. One or more processor readable storage devices according to claim 39, wherein: said access system protects a plurality of resources that are separate from said access system; and said plurality of resources includes said first resource.

41. (Cancelled).

42. (Previously Presented) One or more processor readable storage devices according to claim 39, wherein: said step of authenticating provides a name for said second entity; and said step of authorizing includes the steps of: accessing said name, accessing a user identity profile for said second entity based on said name, accessing a set of one or more authorization rules for said resource, and comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said resource.

43. (Previously Presented) One or more processor readable storage devices according to claim 39, wherein: said authentication credentials correspond to a set of attributes for said first entity; said identification of said second entity corresponds to a set of attributes for said second entity; said step of authorizing is based on one or more of said attributes for said first entity; and said step of authorizing is based on one or more of said

attributes for said second entity.

44. (Previously Presented) One or more processor readable storage devices according to claim 39, wherein said method further comprises the steps of: receiving a request to access a second resource from said first entity after said step of authenticating said first entity, said access system protects said second resource; and authorizing said first entity to access said second resource as said second entity, said step of authorizing said first entity to access said second resource is performed without authenticating said first entity in response to said request to access said second resource.

45. (Currently amended) An apparatus for providing access management that allows for impersonating, comprising:

- a communication interface;

- a storage device; and

- a processing unit in communication with said communication interface and said storage device, said processing unit performs a method comprising the steps of:

- receiving authentication credentials for a first entity and an identification of a second entity at an access system, said access system protects a first resource that is separate from said access system,

- authenticating said first entity based on said authentication credentials for said first entity, said step of authenticating is performed by said access system, and

Art Unit: 2143

authorizing said first entity to access said first resource as said second entity, said step of authorizing is performed by said access system;

wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said second entity, and accessing one or more attributes of said second user identity profile; and said step of authorizing uses said one or more attributes of said second user identity profile.

46. An apparatus according to claim 45, wherein: said access system protects a plurality of resources that are separate from said access system; and said plurality of resources includes said first resource.

47. (Cancelled).

48. (Previously Presented) An apparatus according to claim 45, wherein: said step of authenticating provides a name for said second entity; and said step of authorizing includes the steps of: accessing said name, accessing a user identity profile for said second entity based on said name, accessing a set of one or more authorization rules

for said resource, and comparing attributes of said user identity profile for said second entity to said set of one or more authorization rules for said resource.

Reasons for Allowance

3. 1.(Currently amended) A method for impersonating, comprising the steps of:
receiving authentication credentials for a first entity and an identification of a second entity;

authenticating said first entity based on said authentication credentials for said first entity;

creating a cookie that stores an indication of said second entity if said step of authenticating is performed successfully;

authorizing said first entity to access a first resource as said second entity based on said cookie;

wherein: said authentication credentials include an ID and a password; said step of authenticating includes the steps of:

searching a directory server for a first user identity profile that matches said ID, verifying said password based on said user identity profile, searching said directory server for a second user identity profile that matches said identification of said second entity, and accessing one or more attributes of said second user identity profile; and

said cookie includes said one or more attributes of said second user identity profile.

Art Unit: 2143

4. The dependent claims further limit the independent claims and are considered allowable on the same basis as the independent claims as well as for the further limitations set forth.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "**Comments on Statement of Reasons for Allowance.**"

4. **Claims 1-7, 9-18, 20-24, 26-30, 32-36, 38-40, 42-46 and 48 are allowed.**

Renumbered 1-41.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Jude Jean-Gilles whose telephone number is (571) 272-3914. The examiner can normally be reached between the hours of 9:00 AM to 6:00 PM daily.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, David A. Wiley can be reached on (571) 272-3923. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

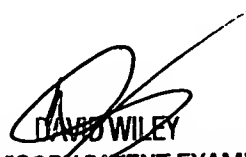
Jude Jean-Gilles

Patent Examiner

Art Unit 2143

JJG

September 25, 2006


DAVID WILEY
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2101